

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

PARAMOUNT PICTURES CORPORATION,	)	
a Delaware corporation,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No.: 05-11588-RWZ
	)	
JOHN DOE,	)	
	)	
Defendant.	)	

**DECLARATION OF CHAD TILBURY IN SUPPORT OF PLAINTIFF'S MOTION FOR  
LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE**

I, Chad Tilbury, declare:

1. I am Director of Worldwide Internet Enforcement for the Motion Picture Association of America, Inc. ("MPAA"), where I have been employed since July 2004. Prior to the MPAA, I spent five years as a Special Agent in the Air Force Office of Special Investigations where I was responsible for computer investigations and operations. I have an M.S. and a B.S. in Computer Science and have also worked as an Artificial Intelligence researcher and a computer security engineer in the defense industry. I submit this declaration in support of Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference.

2. The Plaintiff in this action is a motion picture studio and/or distributor, and is a member, or affiliate or subsidiary of a member, of the MPAA. The MPAA is a trade association whose members include the largest motion picture studios in the United States. Among other things the MPAA investigates the unauthorized reproduction and distribution of copyrighted motion pictures on behalf of its member companies. As Director of Worldwide Internet Enforcement, I am responsible for coordinating the MPAA's worldwide enforcement effort against internet piracy. This includes supervision of our online copyright infringement campaign, identification and development of Internet anti-piracy technologies,

investigations of major online infringers and coordination of Internet anti-piracy efforts around the globe.

3. This declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

**Background**

4. The Internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of people around the world to freely and easily exchange ideas and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data. Unfortunately, the Internet also has afforded opportunities for the wide-scale infringement of copyrighted motion pictures. Once a motion picture has been transformed into an unsecured digital format, it can be copied further and distributed an unlimited number of times over the Internet, without significant degradation in picture or sound quality.

5. To copy and distribute copyrighted motion pictures over the Internet, many individuals use online media distribution systems or so-called "peer-to-peer" ("P2P") networks. P2P networks, at least in their most common form, are computer systems that enable Internet users to: (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the Internet.

6. At any given moment, millions of people around the world unlawfully use these P2P networks to upload (distribute) or download (copy) copyrighted material. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to still other users and so on, so that almost-perfect copies of an infringing file can be distributed to millions of people worldwide with breathtaking speed. Significantly, a person who uses a P2P network is free to use any

alias (or “screen name”) whatsoever, without revealing his or her true identity to other users. Thus, while Plaintiff can observe the infringement occurring on the Internet, it does not know the true name or address of those individuals who are committing the infringement

7. Because the Plaintiff has not authorized their copyrighted motion pictures to be copied or distributed in unsecured formats by means of P2P networks, the copying and distribution of these motion pictures on P2P networks violates the copyright laws.

#### **Plaintiff's Identification of the Doe Defendants**

8. In order to assist Plaintiff in combating copyright infringement on P2P networks, the MPAA and counsel for Plaintiff retained MediaSentry, a company that provides online anti-piracy and copyright protection services and investigations through sophisticated technology and especially developed software programs. (See Decl. of Thomas Carpenter.) Under the direct supervision of counsel, MediaSentry caused searches of several P2P networks to be conducted for infringing copies of motion pictures whose rights are owned by Plaintiff. The search function of the P2P network was used to look for network users who were offering for distribution audiovisual files that were labeled with the names of certain of Plaintiff's copyrighted motion pictures. When a network user was located that was making such files available for distribution, MediaSentry downloaded and retained both the files that were being offered for distribution and other specific information in order to confirm that infringement was occurring and to identify the infringer. (See Decl. of Thomas Carpenter.) In addition, the downloaded audiovisual files were reviewed in order to confirm that the files were in fact copies of substantial portions of motion pictures whose rights are owned by Plaintiff. (See Decl. of R. Christopher Harshman.)

#### **The Need For Expedited Discovery**

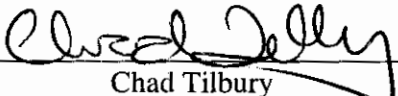
9. Obtaining the identity of copyright infringers on an expedited basis is critical to prosecution of this action and stopping the continued infringement of Plaintiff's copyrighted motion pictures.

10. Without expedited discovery, Plaintiff has no way of serving Defendant with the complaint and summons in this case. Plaintiff does not have Defendant's name, address, e-mail address, or any other way to identify or locate Defendant.

11. Further, service providers have different policies pertaining to the length of time they preserve "logs" which identify their subscribers. Despite requests to preserve the information, some ISPs keep log files of their subscribers' activities for only limited periods of time -- sometimes as little as weeks or even days -- before erasing the data they contain. If an ISP does not have to respond expeditiously to a discovery request, the identification information in that ISP's logs may be erased.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on 7/29, 05, at Encino, CA.

  
Chad Tilbury